NASA Procedural Requirements

NPR 8705.5
Effective Date: July 12, 2004
Expiration Date: July 12, 2009

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Subject: Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects

Responsible Office: Office of Safety and Mission Assurance

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | AppendixA | ALL |

CHAPTER 1: Overview

1.1 Introduction

1.1.1 It is NASA policy to implement structured risk management (RM) processes and use qualitative and quantitative risk assessment techniques to support optimal decisions regarding safety and the likelihood of mission success. This requirement is stated in NPD 8700.1, NASA Policy for Safety and Mission Success.

1.1.2 Probabilistic Risk Assessment (PRA) is a comprehensive, structured, and logical analysis methodology aimed at identifying and assessing risks in complex technological systems. PRA is generally used for low-probability, high-consequence events for which limited statistical data exist. Its application, as discussed in this document, is targeted at risk environments common within NASA that may involve the compromise of safety, inclusive of the potential loss of life, personal injury, and loss or degradation of high-value property that may be found in NASA mission-related programs.

1.1.3 PRA has become a principal analytical methodology for identifying and analyzing technical and safety risk associated with complex systems, projects, and programs. PRA facilitates RM activities by identifying dominant contributors (those events that contribute most to risk) so that resources can be allocated to significant risk drivers and not wasted on items that insignificantly affect overall system risk.

1.1.3.1 PRA provides a framework to quantify uncertainties in events that are important to system safety. By requiring the quantification of uncertainty, PRA informs the decision-makers of the sources of uncertainty and provides information that helps determine the worth of investing resources to reduce uncertainty.

1.1.3.2 PRA differs from reliability analysis in three important respects: (1) PRA tends to focus on the evaluation of system failure while reliability analysis tends to focus on the evaluation of system success; (2) PRA explicitly quantifies uncertainty while reliability analysis nominally considers uncertainty in parameter estimates; and (3) PRA quantifies metrics related to the occurrence of highly adverse consequences (e.g., fatalities, illness, loss of mission), as opposed to narrower system performance metrics such as system reliability. PRA also differs from hazard analysis, which evaluates metrics related to the effects of high consequence and low probability events, treating them as if they have already occurred; i.e., without regard to their likelihood of occurrence. PRA results are directly applicable to resource allocation and other kinds of RM decision-making based on its broader consequence metrics.

1.1.3.3 The PRA process identifies weaknesses and vulnerabilities in a system that can adversely impact safety, performance, and mission success. This information in turn provides insights into viable RM strategies to reduce risk and directs the decision-maker to areas where expenditure of resources to improve design and operation may be more cost-beneficial.

1.1.3.4 The most useful applications of PRA have been in the evaluation of complex systems subject to low-probability and high-consequence scenarios and the evaluation of complex scenarios consisting of chains of events, each of which may adversely impact the system. These complex scenario impacts may include events that separately may appear to be slight or insignificant but collectively can combine and interact to cause high severity consequences.

1.1.4 All PRAs shall be conducted in accordance with this NPR (Requirement 32960).

1.1.4.1 This NPR provides the basic requirements for use of PRA in NASA programs and projects.

1.1.4.2 A companion document to this NPR, the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf, provides further details on PRA methodology for aerospace applications. Many references will be made to this companion document for practical advice on performing PRAs.

1.2 When to Use PRA

1.2.1 NASA program and project managers shall use the criteria in paragraph 1.2.3, Table 1, and paragraph 1.2.4 to determine when a PRA must be conducted and the scope to be implemented (Requirement 32964).

1.2.2 The PRA approach for each project shall be described in the project's risk management plan and submitted for Governing Program Management Committee (GPMC) review and approval at the project formulation decision milestone (Requirement 32965).

1.2.3 Levels of PRA

1.2.3.1 Full Scope PRA

1.2.3.1.1 A "full-scope" analysis contains all major PRA components as outlined in chapter 2 of this NPR. Decision-making for projects involving complex systems in high-stakes programmatic contexts shall be supported by a full-scope PRA with consideration of uncertainty (Requirement 32969).

1.2.3.1.2 Full-scope PRAs address all applicable end states that lead to failure to meet safety and mission objectives. These end states include, but are not limited to, loss of crew, when a crew is part of the mission; accidental exposure to toxic or hazardous materials leading to potential illness or death of public or ground- or space-based personnel; loss of ground-based facilities; loss of space-based facilities or modules; mission abort; loss of mission; and mission reconfiguration.

1.2.3.1.3 Completeness of scenarios is an important consideration in a full-scope PRA. Uncertainty analysis shall be performed to provide the decision-maker with a full appreciation of the overall degree of uncertainty about the PRA results and an understanding of which sources of uncertainty are critical to the results that guide decisions (Requirement 32972).

1.2.3.2 Limited-Scope PRA

1.2.3.2.1 A "limited-scope" PRA applies the steps outlined in chapter 2 of this NPR with the same general rigor as a full-scope PRA but focuses on some of the mission-related end states of specific decision-making interest, instead of all applicable end states.

1.2.3.2.2 The scope is limited and is defined on a case-by-case basis, so that the results can provide specific answers to pre-identified mission-critical questions and safety concerns, rather than the assessment of all relevant risks.

1.2.3.2.3 Similar to a "full-scope" PRA, sources of uncertainties that have a strong effect on the limited-scope PRA results and insights shall be identified and quantified (Requirement 32976).

1.2.3.3 Simplified PRA

1.2.3.3.1 A "simplified" PRA applies essentially the same process outlined in chapter 2 of this NPR but identifies and quantifies major (rather than all) mission risk contributors (to all end states of interest) and generally applies to systems of lesser technological complexity or systems having less available design data than those requiring a full-scope PRA. Thus, a simplified PRA contains a reduced set of scenarios or simplified scenarios designed to capture only essential, sometimes top level, mission risk contributors.

1.2.3.3.2 In a simplified PRA, the sources of uncertainties that have the strongest effects on the PRA results shall be identified and, in cases where they affect the management decision process, shall be quantified (Requirement 32979).

Table 1. Criteria for Selecting the Scope of a Probabilistic Risk Assessment (PRA)

CONSEQUENCE CATEGORY	CRITERIA / SPECIFICS	NASA PROGRAM/PROJECT (Classes and/or Examples)	PRA SCOPE

Human Safety and Health	Public Safety	Planetary Protection Program Requirement	Mars Sample Return Missions	**F**
		White House Approval (PD/NSC-25)	Nuclear Payloads (e.g., Cassini, Ulysses, Mars 2003)	**F**
		Space Missions with Flight Termination Systems	Launch Vehicles	**F**
	Human Space Flight		International Space Station	**F**
			Space Shuttle	**F**
			Human Space Experiments	**F**
			Project Constellation	**F**
Mission Success (for non?human rated missions)	High Strategic Importance / High Value Strategic Property / High Cost Projects		Mars Program	**F**
	High Schedule Criticality		Launch Window (e.g., planetary missions)	**F**
	All Other Missions		Earth Science Missions (e.g., EOS, QUICKSCAT, specific payloads)	**L/S**
			Space Science Missions (e.g., SIM, HESSI, specific payloads)	**L/S**
			Technology Demonstration/Validation (e.g., EO-1, Deep Space 1)	**L/S**
			Medium to Low Cost Projects	**L/S**

***Key:**

F - Full scope PRA as defined in paragraph 3.2.1.

L/S - Limited-scope or simplified PRA should be performed or altogether waived, at the direction of the program/project, as defined in paragraph 3.2.2 and 3.2.3.

1.2.4 Factors to Consider Regarding the Level of PRA.

1.2.4.1 Unlike a full-scope PRA, the complete set of scenarios is not of essence in either a limited-scope or a simplified PRA.

1.2.4.2 Considerations of program risk associated with schedule, performance, technology, and cost should be included for both full- and limited-scope PRAs but, perhaps, in separate analyses.

1.3 Documenting PRA Decisions

1.3.1 After determining the level at which the PRA shall be conducted, the program or project manager shall

document the PRA decision and its basis in the program/project risk plan (Requirement 32984).

1.3.2 The program or project manager shall brief the GPMC on the PRA decision and the rationale during the formulation phase of the program or project (Requirement 32985). (See NPR 1000.3, The NASA Organization, paragraph 6.6.)

1.3.3 Any disputes concerning the PRA decision and level of implementation shall be elevated to the next level of Program Management Committee (Requirement 32986).

1.4 Implementation Responsibility

1.4.1 Enterprise Associate Administrators

1.4.1.1 NPD 8700.1, NASA Policy for Safety and Mission Success, states that Enterprise Associate Administrators and program/project managers are responsible for assuring that appropriate Agency safety, reliability, maintainability, quality, and RM policies, plans, techniques, procedures, and standards are implemented.

1.4.1.2 Towards that end, Enterprise Associate Administrators shall:

a. Ensure that appropriate resources (funding, personnel, methods, and software applications) are made available for PRA (Requirement 32991).

b. Ensure that technical quality is maintained throughout the PRA effort (Requirement 32992).

c. Ensure that PRA methodology and results are effectively transferred to appropriate NASA personnel who are not directly involved in conducting the PRA (Requirement 32993) .

d. Ensure that formal PRA awareness training and methodology training are provided periodically to managers and practitioners (Requirement 32994).

e. Ensure that PRA requirements are appropriately implemented on contracts (Requirement 32995).

1.4.2 Associate Administrator for Safety and Mission Assurance

1.4.2.1 The Associate Administrator for Safety and Mission Assurance is the lead for PRA policy, procedures, guidelines, technical training content, and tools throughout NASA. The Associate Administrator for Safety and Mission Assurance will continually evaluate and adopt best available PRA methods, practices, applications, software, and standards for use in NASA PRA efforts.

1.4.2.2 Further, the Associate Administrator for Safety and Mission Assurance shall:

a. Develop, coordinate, publish, disseminate, explain, interpret, and maintain NASA PRA policy and procedures and assure their correct implementation at Headquarters and at the Centers (Requirement 32999).

b. Have primary responsibility for developing criteria and guidelines for the use of PRA results in management decision-making (Requirement 33000).

c. Provide PRA functional leadership, mentoring, technical direction, and consultation on methodology (on how to conduct a PRA), tools, and oversight Agencywide (Requirement 33001).

d. Provide corporate leadership and establish a community of practice for the exchange of PRA-related information, best practices, and lessons learned across programs/projects, Centers, government agencies, and international partners (Requirement 33002) .

e. Assess and assure that PRAs are correctly initiated, conducted, and utilized within Enterprises and programs/projects (Requirement 33003).

f. Enable, facilitate, and organize the development of a PRA "corporate memory" (Requirement 33004). This includes:

(1) Assist in the maintenance of PRAs and their updating, as necessary (Requirement 33005).

(2) Collect, from NASA programs/projects, documentation of all PRAs conducted, including their scope, PRA models developed and data used, preliminary and final reports issued, and the results of independent or peer reviews (Requirement 33006).

(3) Assure the availability of all approved PRA documentation for present and future programs/projects (Requirement 33007).

g. Designate and provide or assist in acquiring state-of-the-art and verified PRA methods, computer applications, and training for NASA personnel (Requirement 33008).

h. Organize and coordinate peer reviews of PRA work performed, if deemed appropriate, and assure the

implementation of peer review recommendations and the overall credibility of PRA efforts and results (Requirement 33009).

i. Contribute to and approve program/project Level 1 (NASA Headquarters-level program management) probabilistic risk assessment requirements; and provide oversight and advice on Level 2 (NASA Center-level program management) and lower-level probabilistic risk assessment requirements (Requirement 33010).

j. Assure that PRA results are provided in an acceptable, useable form (e.g., medians, means, lower and upper uncertainty bounds, and risk drivers) and are accurately represented and communicated to NASA management (Requirement 33011).

k. Guide and direct the use of PRA during the system development life cycle to improve design, operation, and upgrade (Requirement 33012).

l. Enable, facilitate, and organize a central resource and repository of PRA tools, methods, and data, and the transfer of PRA technology to NASA Civil Service personnel (Requirement 33013).

m. Assist in the acquisition and verify the credentials of PRA practitioners, both for Civil Service personnel and for supporting contractors or consultants (Requirement 33014).

1.4.3 Center Directors shall ensure that their Safety and Mission Assurance (SMA) and Engineering organizations acquire and maintain expertise in PRA necessary to support Center-based programs/projects (Requirement 33015).

1.4.4 Center Directors, Center SMA Directors, and program/project SMA Directors shall assist Center-based programs/projects in conducting required PRAs; i.e., provide required resources, training, tools, technical advice, or assistance in obtaining competent support services (Requirement 33016).

1.4.5 Program/project managers and other decision-makers shall conduct and use PRA with the best state-of-practice methods and data to support management decisions to improve safety and performance (Requirement 33017). (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapters 7 and 12.)

1.4.5.1 Program/project managers shall document PRA decisions, justifications and plans for implementing and conducting PRAs in program/project risk management plans (Requirement 33018).

1.4.5.2 The program or project manager shall brief the GPMC on the PRA decision and the rationale during the formulation phase of the program or project (Requirement 33019).

1.4.5.3 Program/project managers shall maintain and safeguard records resulting from PRAs in accordance with the guidelines in NPR 1441.1, NASA Records Retention Schedule ((Requirement 33020).

1.4.5.4 Program/project managers shall adequately and clearly communicate PRA results and insights that explicitly include initial assumptions, residual uncertainties, and significant risk drivers to all involved program/project staff and management, and ensure that the PRA results and insights, as well as their implications regarding systems design, operation, and upgrade, are reviewed, analyzed, properly interpreted, and understood (Requirement 33021). (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 13.)

1.4.5.5 Program/project managers shall update design, operating, and implementation plans to reflect insights from PRA and use the insights gathered from PRA to reinforce or modify existing relevant management decisions or to generate new management decisions (Requirement 33022). (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 13.)

1.4.5.5.1 If the residual risk, as shown through the use of PRA, is deemed unacceptable as defined by program requirements, the program/project manager shall consider modifying the project through design, operation, upgrade, and maintenance, and implement management decisions to reduce risk to an acceptable level as defined at the appropriate level of the Agency; i.e., Headquarters, Center, Enterprise, program, or project, as appropriate (Requirement 33023).

1.4.5.5.2 Residual risk is defined as the risk that remains or is introduced following the implementation of prevention and mitigation measures and controls.

1.4.6 NASA shall, through prudent hiring, professional development, and mentoring, increase and maintain its capability to conduct, understand, and use PRA in support of a program/project life cycle (Requirement 33025).

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | AppendixA | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS